

PATENT COOPERATION TREATY

REC'D 12 DEC 2005

PCT

WIPO

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference 8758PCT	FOR FURTHER ACTION		See Form PCT/IPEA/416
International application No. PCT/US04/21621	International filing date (day/month/year) 07 July 2004 (07.07.2004)	Priority date (day/month/year) 07 July 2003 (07.07.2003)	
International Patent Classification (IPC) or national classification and IPC IPC(7): G06F 12/14 and US CL: 713/185			
Applicant CRYPTOGRAPHY RESEARCH			
<p>1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>4</u> sheets, including this cover sheet.</p> <p>3. This report is also accompanied by ANNEXES, comprising:</p> <p>a. <input checked="" type="checkbox"/> (sent to the applicant and to the International Bureau) a total of <u>1</u> sheets, as follows:</p> <p><input type="checkbox"/> sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).</p> <p><input type="checkbox"/> sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.</p> <p>b. <input type="checkbox"/> (sent to the International Bureau only) a total of (indicate type and number of electronic carrier(s)) _____, containing a sequence listing and/or tables related thereto, in electronic form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).</p> <p>4. This report contains indications relating to the following items:</p> <p><input checked="" type="checkbox"/> Box No. I Basis of the report</p> <p><input type="checkbox"/> Box No. II Priority</p> <p><input type="checkbox"/> Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p><input checked="" type="checkbox"/> Box No. IV Lack of unity of invention</p> <p><input checked="" type="checkbox"/> Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p><input type="checkbox"/> Box No. VI Certain documents cited</p> <p><input type="checkbox"/> Box No. VII Certain defects in the international application</p> <p><input type="checkbox"/> Box No. VIII Certain observations on the international application</p>			
Date of submission of the demand 02 February 2005 (02.02.2005)	Date of completion of this report 02 December 2005 (02.12.2005)		
Name and mailing address of the IPEA/US Mail Stop PCT, Attn: IPEA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (571) 273-3201	<p>Authorized officer <u>Emmanuel Moise</u></p> <p>Emmanuel Moise</p> <p>Telephone No. 305-3900</p>		

Box No. I Basis of the report

1. With regard to the language, this report is based on:

the international application in the language in which it was filed.

a translation of the international application into English, which is the language of a translation furnished for the purposes of:

- international search (under Rules 12.3 and 23.1(b))
- publication of the international application (under Rule 12.4(a))
- international preliminary examination (under Rules 55.2(a) and/or 55.3(a))

2. With regard to the elements of the international application, this report is based on (*replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report*):

the international application as originally filed/furnished

the description:

pages 1-120 as originally filed/furnished
 pages* received by this Authority on
 pages* NONE received by this Authority on

the claims:

pages 122 and 123 as originally filed/furnished
 pages* NONE as amended (together with any statement) under Article 19
 pages* 121 received by this Authority on 14 July 2005 (14.07.2005)
 pages* NONE received by this Authority on

the drawings:

pages 1-5 as originally filed/furnished
 pages* NONE received by this Authority on
 pages* NONE received by this Authority on

a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing.

3. The amendments have resulted in the cancellation of:

the description, pages _____
 the claims, Nos. _____
 the drawings, sheets/figs _____
 the sequence listing (*specify*): _____
 any table(s) related to the sequence listing (*specify*): _____

4. This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

the description, pages _____
 the claims, Nos. _____
 the drawings, sheets/figs _____
 the sequence listing (*specify*): _____
 any table(s) related to the sequence listing (*specify*): _____

* If item 4 applies, some or all of those sheets may be marked "superseded."

Form PCT/IPEA/409 (Box No. I) (April 2005)

Box No. IV Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees the applicant has, within the applicable time limit:
 - restricted the claims.
 - paid additional fees.
 - paid additional fees under protest, and, where applicable, the protest fee
 - paid additional fees under protest but the applicable protest fee was not paid
 - neither restricted the claims nor paid additional fees
2. This Authority found that the requirement of unity of invention is not complied with and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.
3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is:
 - complied with.
 - not complied with for the following reasons:

Group 1, claims 1-4 and 11, drawn to a method for limiting access to non-volatile digital storage contained in a device executing instructions in a Turing-complete interpreter.

Group 2, claims 5-7, drawn to a digital optical storage medium containing encrypted audiovisual content playback on any of a plurality of device architectures.

Group 3, claims 8-10, drawn to an automated method for enabling a playback device containing a non-volatile memory to determine whether permission to use the digital optical disk media has been revoked.

The inventions listed as groups 1-3 do not relate to a single general inventive concept under PCT Rule 13.1 because under PCT Rule 13.2 they lack the same or corresponding special technical features for the following reasons: Group 1 claim limitations directed to access control via authentication of a hash value of executables, Group 2 claim limitations directed to an optical disk with an executable that upon playback determines a security weakness of the playback device, Group 3 claim limitations directed to limiting access to a digital storage medium via determining if an instance of permission to utilize the medium has been revoked by comparison of a read identifier with a revocation list.

No generic linking claim is found.

The 3 claim groups are independent and distinct from one another as per MPEP Sec. 802.21 and within the meaning of 35 USC 121.

4. Consequently, this report has been established in respect of the following parts of the international application:

- all parts
- the parts relating to claims Nos. 1-4, 11

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/US04/21621

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims <u>1-4, 11</u>	YES
	Claims <u>NONE</u>	NO
Inventive Step (IS)	Claims <u>1-4, 11</u>	YES
	Claims <u>NONE</u>	NO
Industrial Applicability (IA)	Claims <u>1-4, 11</u>	YES
	Claims <u>NONE</u>	NO

2. Citations and Explanations (Rule 70.7)

Claims 1-4 the criteria set out in PCT Article 33(2)-(3), because the prior art does not teach or fairly suggest:

The closest prior art in the field, Schneck et al., US 6,314,409 B2, when taken singly and in reasonable combination with the other prior art, does not teach the features found in the independent claims of authenticating an access request by forming a cryptographic hash of executable instructions sent with a request for access to a portion of a storage medium at a receiving device via authenticating the hash, all in the manner of the applicant as taught by the Specification.

----- NEW CITATIONS -----

IPPEAVUS
PCT/US2014/221421 - 14272015

We claim

1. A method for regulating access to nonvolatile digital storage contained in a device executing instructions in a Turing-complete interpreter, said method comprising

5 (a) receiving a request from said instructions being executed, wherein said request specifies:

- (i) a portion of said storage for which access is requested, and
- (ii) a plurality of additional executable instructions;

10 (b) applying a cryptographic hash function to said additional executable instructions to obtain a hash value;

(c) authenticating said hash value; and

(d) provided that said authentication is successful, enabling access by said instructions being executed to said requested portion of said storage while executing said additional executable instructions.

15

2. The method of claim 1 wherein said step of authenticating comprises comparing said hash value with a hash value stored in said nonvolatile storage.

20 3. The method of claim 1 wherein said step of authenticating comprises verifying a digital signature provided by said instructions being executed.

4. The method of claim 1 wherein said request includes a pointer to said additional executable instructions in memory accessible by said instructions being executed and contained in said device.

25

5. A digital optical disc medium containing encrypted audiovisual content for playback on any of a plurality of device architectures, said digital optical disc medium comprising program logic configured to:

(a) identify at least one characteristic of a device executing said program logic;